MANRS Community Report 2023

January 2024

Table of Contents

1. MANRS at a Glance

2. About Us

Mutually Agreed Norms for Routing Security (MANRS) is a global, community-driven initiative. In 2014, a small group of network operators recognized the need to join forces to improve the security and resilience of the Internet's global routing system. With support from the Internet Society, MANRS was born.

Within a decade, MANRS has grown from nine original operators to a community of more than 1,000 participants. The MANRS community comprises network operators,[1] Internet exchange points (IXPs),[2] content delivery network (CDN) and cloud providers,[3] and equipment vendors[4] who have committed to taking MANRS actions[5] and reducing common routing threats. MANRS would not have been possible without the dedication of these participants and partner organizations.[6]

Together, the MANRS community is driving the global adoption of MANRS actions and improvements in routing security. Efforts toward achieving this goal include providing reliable tools[7] for compliance and measurement, such as the MANRS Observatory;[8] building capacity of network engineers through tutorials, courses, and workshops;[9] and promoting training, research, and policy analysis through the Mentors and Ambassadors[10] program.

In accordance with the MANRS Community Charter,[11] the MANRS Steering Committee[12] was established in 2021, with elections held annually. It comprises individuals elected by the MANRS community to lead the community toward collective responsibility for the resilience and security of the Internet's global routing system.

Since the inception of MANRS, the Internet Society has served as the secretariat, providing financial, staffing, and operational support. From 1 January 2024, MANRS' secretarial and operational functions will transition[13] to the Global Cyber Alliance (GCA) as part of a partnership between the Internet Society and GCA. The Internet Society will continue to focus on funding and support through training and global advocacy. The MANRS Steering Committee has endorsed this partnership and transition. Together, the Internet Society and GCA are committed to maintaining and expanding the vision of MANRS, and increasing the awareness and uptake of MANRS actions.

If you want to learn how your organization can support MANRS, please visit our website[14] or contact us.[15]

---

[1] https://www.manrs.org/netops/

[2] https://www.manrs.org/ixps/

[3] https://www.manrs.org/cdn-cloud-providers/

[4] https://www.manrs.org/equipment-vendors/

[5] MANRS actions are the compulsory and recommend actions that MANRS participants should be taking to improve the security and resilience of the Internet global routing system. There are defined actions for network operators, IXPs, CDN and cloud providers, and equipment vendors.

[6] Partner organizations do not operate a network but actively support MANRS goals. https://www.manrs.org/about/partners/

[7] https://www.manrs.org/resources/

[8] https://www.manrs.org/manrs-observatory/

[9] https://www.manrs.org/resources/training/

[10] https://www.manrs.org/champions/

[11] https://www.manrs.org/about/governance/community-charter/

[12] https://www.manrs.org/about/governance/steering-committee/

[13] https://www.manrs.org/2023/11/achieving-greater-heights-for-manrs/

[14] https://www.manrs.org/join/

[15] https://www.manrs.org/about/contact/

10 YEARS OF MANRS

1000+ MANRS Participants
2023

MANRS+ Working Group Established
2022

MANRS Steering Committee Established

Equipment Vendor Program Launched
2021

First Cohort of Mentors and Ambassadors

CDN and Cloud Provider Program Launched
2020

MANRS Observatory Launched
2019

100 MANRS Participants

IXP Program Launched
2018

MANRS Project Study Report Published
2017

40 MANRS Participants
2016

MANRS Implementation Guide Prepared
2015

Launch of MANRS
2014

3. Our Impact in 2023

MANRS Participants are Setting the Standard for Global Routing Security

Creating and validating Route Origin Authorizations (ROAs) using the Resource Public Key Infrastructure (RPKI) system are essential actions to ensure routing security. MANRS participants have a much higher compliance rate, with 66% of participants with valid ROAs, compared with 34% of autonomous systems with valid ROAs globally. Similarly, the deployment rate of Route Origin Validation (ROV) is much higher among MANRS participants, with 16% of their traffic filtering based on ROV, compared with 5% globally.
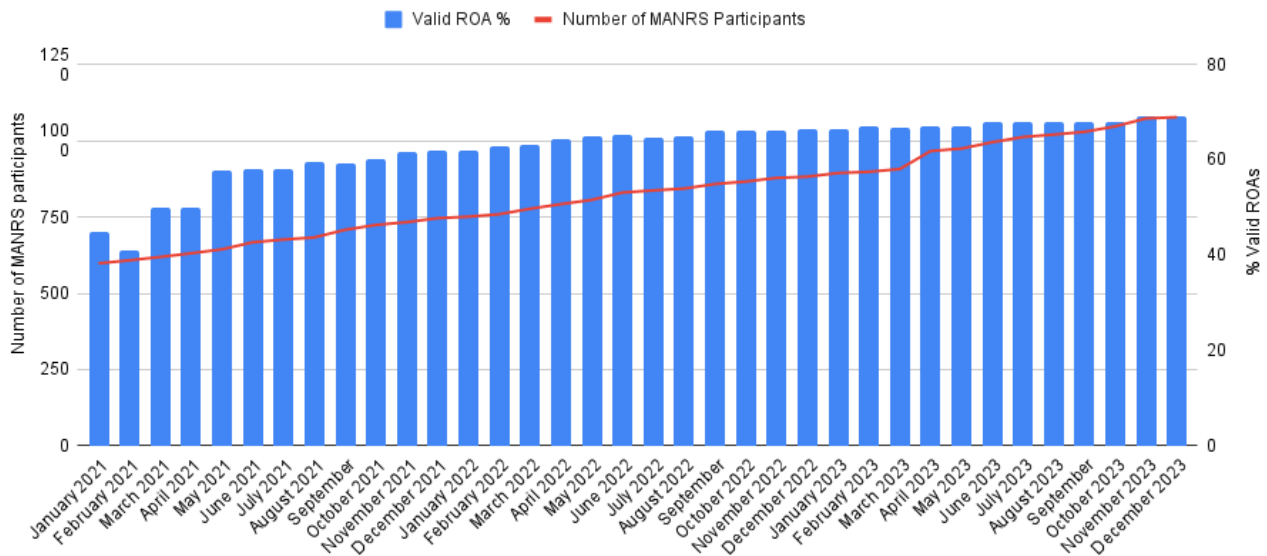
Figure 1 The Percentage of MANRS Participants with Valid ROAs, 2021-2023.

The overall figure, however, masks regional disparities, and it is worth noting that improvement in routing security is needed in most of Africa and Eastern Asia.

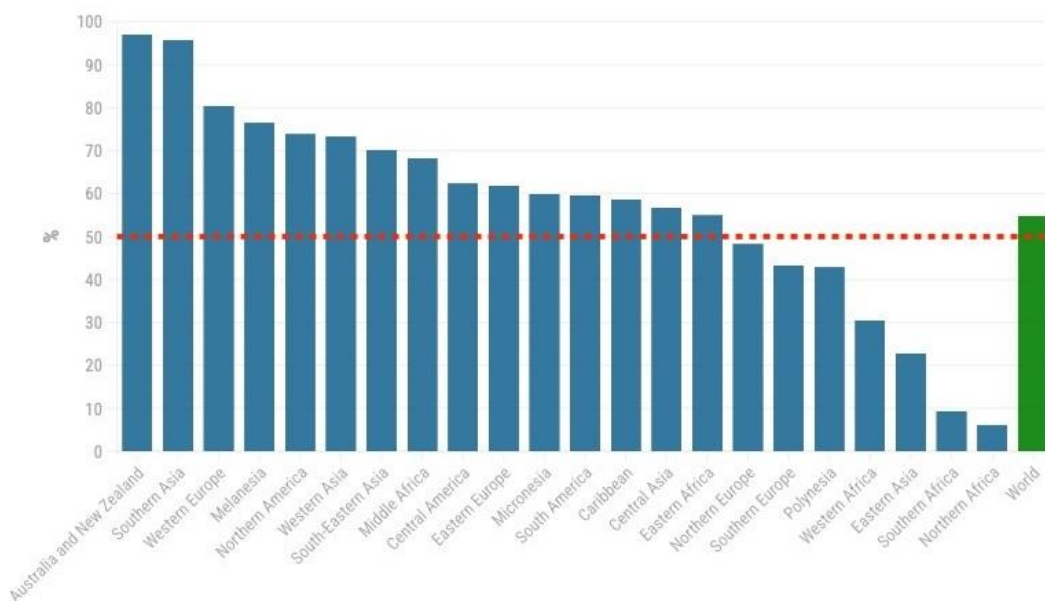**Figure 2. Regional Variation in Routing Security: IPv6 Address Space Covered by ROA, December 2023.**

Figure 2 Regional Variation in Routing Security: IPv6 Address Space Covered by ROA, December 2023.

MANRS+ Working Group Develops More Stringent Requirements and Auditing Guidelines, Paving the Way for Value Chain Security

In 2022, the community formed the MANRS+ Working Group[16] to create a second, elevated tier of MANRS participation for organizations that comply with more stringent requirements and auditing. Its charter[17] describes the working group's intention to create a significantly higher value proposition for a subset of existing MANRS participants. It will be based on a credible quality mark that customers recognize. This quality mark and its implementation and conformance requirements assume better alignment with customer needs, leading to better security assurance.

The MANRS+ Working Group, co-chaired by Matt Davy (Visa) and Andrei Robachevsky (Internet Society), met monthly throughout 2023. Informed by a survey,[18] the MANRS+ concept[19] and a set of control and auditing requirements[20] were developed. In 2024, the working group will focus on developing detailed audit requirements, including descriptions of the audit metrics and creating an extended measurement framework and infrastructure.

MANRS' Community Elects Three Steering Committee Members

The third election[21] of the MANRS Steering Committee for three seats attracted eight high-caliber and diverse candidates.[22] The following three members were elected:

- Arturo Sevrin, Google (re-elected for a second term)
- Nick Hilliard, INEX (re-elected for a second term)
- Nicolas Fiumarelli Santana, LACNIC

Together, they join six other steering committee members[23] to: make recommendations on MANRS actions and minimum conformance criteria; supervise the auditing process for new applicants; handle the appeals process from applicants that have been refused approval; make recommendations on the suspension and termination of organizations from MANRS participation that fail to meet the minimum conformance criteria; supervise the incident handling processes; and appoint MANRS advisors who can offer specialist advice or act as liaisons with other communities.

MANRS Readiness Scores Made Public for Network Operator Participants

As recommended by the MANRS Steering Committee, the MANRS readiness scores (Actions 2—4) for network operator participants[24] were made public in July[25] to align with the community's objectives to:

- Raise awareness of routing security problems and encourage networks to implement best current practices to address them.
- Improve transparency and credibility of the MANRS initiative.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.

---

[16] https://www.manrs.org/about/manrs-working-group/

[17] https://www.manrs.org/about/manrs-working-group-charter/

[18] https://www.manrs.org/2023/08/survey-shows-enterprises-value-routing-security-may-underestimate-their-ability-to-influence-vendors/

[19] https://www.manrs.org/about/manrs-working-group/manrs-concept/

[20] https://www.manrs.org/wp-content/uploads/2023/12/MANRSPlus_Controls.pdf

[21] https://www.manrs.org/2023/11/new-manrs-steering-committee-members-elected/

[22] https://www.manrs.org/about/governance/2023-steering-committee-candidates/

[23] https://www.manrs.org/about/governance/steering-committee/steering-committee-members/

[24] https://www.manrs.org/netops/participants/

[25] https://www.manrs.org/2023/06/manrs-readiness-scores-to-be-made-public-for-network-operator-participants/

The MANRS readiness scores[26] indicate the degree of participants' conformance to MANRS actions. MANRS participants have been able to view readiness scores for all participants via the MANRS Observatory since 2019. Network operator participants have also received individual conformance reports with their scores and any changes to the score since the previous report at the start of each month.

The MANRS team continues to improve the accuracy and visibility of these scores, including adding them to the monthly conformance reports, validating incidents, and improving the quality of the data used to calculate the scores. We are now at a point where the scores provide an adequate analysis of MANRS participants' compliance toward MANRS actions 2, 3, and 4. The MANRS team is refining the score's accuracy for action 1[27] before making this public in 2024.

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
AIRNET S.R.L.S.	28th Jul 2021	IT	209301	✔		100%	100%	100%
Airs Project Private Network	26th Jan 2023	CN, HK, JP, US, EU	142553	✔		100%	100%	100%
Airtek Solutions C.A	26th Apr 2023	VE	61461	✔		100%	100%	64%
AlagoinhasTelecom	5th Sep 2022	BR	268349	✔	No data	100%	100%	100%
Alaska Communications	6th Apr 2020	US	7782	✔		100%	100%	63%
Alfa Service	7th Apr 2021	IT	209102	✔	No data	100%	100%	100%
Algar Telecom	25th Aug 2018	BR	16735, 53006, 27664	✔		50%	98%	0%
All Points Broadband	25th Apr 2023	US	18786, 393713	✔		100%	100%	90%
Alt Telecom	10th Jul 2019	CA, US	21659	✔		100%	100%	67%
Alternativa Internet	11th Nov 2022	BR	264459	✔		100%	100%	0%

Figure 3 Screenshot of Selected Network Operators' Readiness Scores.

MANRS Community Reach and Engagement Strengthened

In 2023, the MANRS team and MANRS mentors and ambassadors presented at nearly 50 in-person and virtual events across six continents and held a record five MANRS community meetings, including the first community-led meeting in the Latin America region. The five meetings were held at APRICOT 2023,[28] RIPE 86,[29] AFPIF 2023,[30] LACNIC 40/LACNOG 2023,[31] and RIPE 87.[32]

---

[26] https://www.manrs.org/manrs-observatory/measurement-framework/

[27] https://www.manrs.org/2023/12/the-road-to-publishing-action-1-netops-scores/

[28] https://www.manrs.org/event/manrs-community-meeting-10/

[29] https://www.manrs.org/event/manrs-community-meeting-11/

[30] https://www.manrs.org/event/manrs-community-meeting-12/

[31] https://www.manrs.org/event/manrs-community-meeting-13/

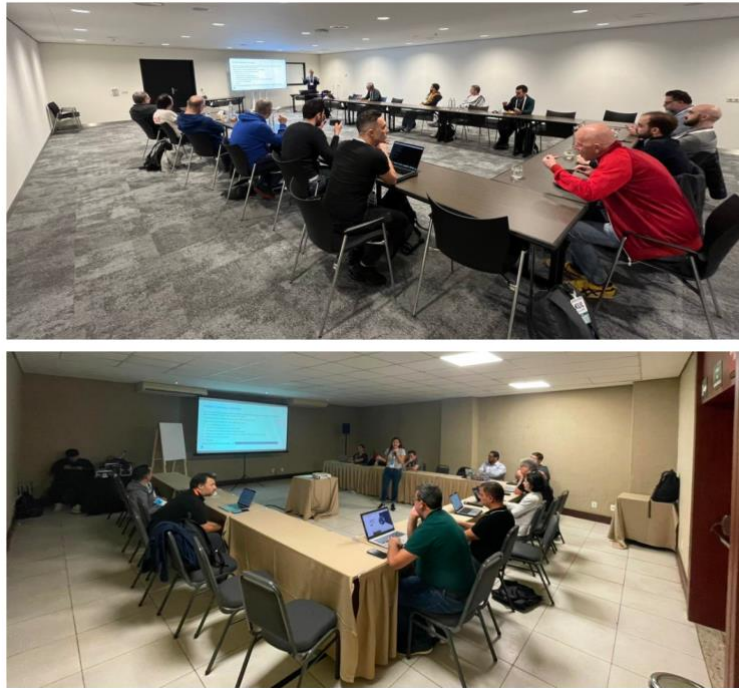[32] https://www.manrs.org/event/manrs-community-meeting-14/

Figure 4 MANRS Community Meetings at RIPE 86 and LACNIC 40/LACNOG 2023.

The feature event for the year was the Routing Security Summit[33] in July, which sought to build on and broaden the scope of RPKI Week.[34] The Routing Security Summit brought together[35] partners from across the Internet routing ecosystem to answer questions about routing security and the MANRS initiative, discuss successes with implementing routing security measures such as RPKI, and share ideas on how to build awareness about routing security among not just the technical community but the wider Internet community. The summit featured four tutorials and six panel sessions, highlights of which included:

- Routing Security as Supply Chain Security: Threats and Opportunities[36]

- It Takes a Community: Exchanging Routing Security Best Practices[37]

- The Role of Computer Security Incident Response Teams (CSIRTS) in Routing Security[38]

- ROV Research Review[39]

Figure 5 Overview of the Routing Security Summit.

---

[33] https://www.manrs.org/event/routing-security-summit-2023/

[34] https://www.manrs.org/event/rpki-week-2022/

[35] https://www.manrs.org/2023/08/enterprises-connectivity-providers-and-governments-must-work-together-to-increase-routing-security/

[36] https://youtu.be/SPHSTnSEDfg

[37] https://youtu.be/MT6HphvTlqo

[38] https://youtu.be/whN0vAta0RM

[39] https://youtu.be/5hwHwQ3UTvI

MANRS Step Up Engagement with Governments

The MANRS team and some participants are working with [governments](#)[40] to improve routing hygiene in their countries by participating in government workshops and submitting public comments. The decisions these governments make will significantly impact the future of the globally distributed Internet routing system.

In the United States, the Federal Communications Commission (FCC) held a [Border Gateway Protocol (BGP) Security Workshop](#)[41] in July. At the workshop, MANRS participants highlighted the importance of addressing BGP vulnerabilities and securing Internet routing. Also in July, the Biden-Harris Administration published the National Cybersecurity Strategy Implementation Plan, which identifies "collaborating with key stakeholders to drive secure Internet routing" as a key action item. The United States Federal Government is considering how to improve the routing security of its own networks. [Comments](#)[42] were submitted in response to the FCC's notice of inquiry on secure Internet routing.

In the Netherlands, the Dutch government announced that it will upgrade the routing security of government networks by adopting the RPKI standard before the end of 2024. Through its "comply or explain" initiative, governmental departments must deploy RPKI or adequately explain why they cannot comply. During a panel session moderated by the Internet Society at the [Internet Governance Forum 2023](#),[43] this approach was clarified and promoted.

In an effort to further engage with governments, the MANRS team organized a session at the 2023 Routing Security Summit on "[working with governments to progress routing security](#)".[44]

Strategic Advocacy in Targeted Regions and Countries Continued Strong

The MANRS community continued to tirelessly advocate for MANRS across different regions and countries throughout 2023. The MANRS community participated in several events in various regions to raise awareness about MANRS, advocate for participation in MANRS actions, and share knowledge and best practices. The events across six regions include, among others:

- **Africa:** AFPIF 2023 (Ghana), 2023 FIRST and AfricaCERT Symposium (Rwanda), and Africa Internet Summit 2023 (South Africa).

- **Asia-Pacific:** [APNIC 56](#) (Japan),[45] APRICOT 2023 (Philippines), [SANOG 39](#) (Bangladesh),[46] [SANOG 40](#) (Sri Lanka),[47] TWNIC (Taiwan), and VNNIC (Vietnam).

- **Europe:** 39th EURO-IX Forum (Czech Republic), RIPE 86 (Netherlands), and RIPE 87 (Italy).

- **Latin America:** [LAC Peering Forum 2023 and LACNIC 39](#) (Mexico),[48] and LACNIC 40 and LACNOG 2023 (Brazil).

- **Middle East:** MENOG 23 (Saudi Arabia).

- **North America:** [ARIN 52](#),[49] FS-ISAC 2023 FinCyber Today Summit, ISC2 Security Congress, NANOG 88, NANOG 89, and ONUG Fall 2023.

---

[40] https://www.manrs.org/2023/09/good-manrs-make-an-impression-on-governments/

[41] https://www.manrs.org/2023/08/us-fcc-workshop-highlights-routing-security/

[42] https://www.fcc.gov/ecfs/document/10303534317884/1

[43] https://www.intgovforum.org/en/content/igf-2023-open-forum-57-procuring-modern-security-standards-by-governmentsindustry

[44] https://youtu.be/9I6f31VFbMo

[45] https://www.manrs.org/2023/10/reflecting-on-the-value-of-manrs/

[46] https://www.manrs.org/2023/05/south-asia-bangladesh-leading-routing-completeness/

[47] https://www.manrs.org/2023/11/bcp-185-is-a-must-do/

[48] https://www.manrs.org/2023/08/routing-security-is-a-top-priority-for-lac-ixps/

[49] https://www.manrs.org/2023/11/the-challenges-of-rpki-roa-diffusion-in-research-and-education/

Figure 6 MANRS Participation at Various Events.

Global Engagement Online Also Continued Strong

The MANRS Blog published 53 posts[50] in 2023, 20 of which came from community members, including MANRS mentors and ambassadors. In addition, there were five RPKI deployment case studies from MANRS participants—Amazon Web Services,[51] Digital Ocean,[52] IPXO,[53] NYSERNet,[54] and Verisign.[55] Sharing lessons and success from the community is an important component of MANRS. We welcome any suggestions on posts and resources for the MANRS Blog and website.

An equally important and popular resource is the incident investigations that MANRS researchers provide. These included unpacking the first route leak prevented by ASPA and analyzing the BGP route leak at Angola Cables that slowed connectivity for many Australians. Drawing attention to these incidents provides concrete examples of the importance of implementing MANRS actions.

MANRS social media channels on Facebook,[56] LinkedIn,[57] X,[58] and YouTube[59] allow community members to connect and share their successes, challenges, and opinions. By the end of 2023, we had a total of 4,495 followers on X (289 joined in 2023), 2,493 followers on LinkedIn (702 joined in 2023), and 509 followers on Facebook (149 joined in 2023).

---

[50] https://www.manrs.org/blog/

[51] https://www.manrs.org/2023/10/coordination-key-to-largest-rpki-deployment/

[52] https://www.manrs.org/2023/03/how-digitalocean-became-manrs-compliant/

[53] https://www.manrs.org/2023/09/route-origin-authorization-enhancing-network-security-and-unveiling-critical-insights/

[54] https://www.manrs.org/2023/02/rpki-deployment-case-study-nysernet/

[55] https://www.manrs.org/2023/06/verisigns-path-to-rpki/

[56] https://www.facebook.com/RoutingMANRS/

[57] https://www.linkedin.com/company/routingmanrs

[58] https://twitter.com/RoutingMANRS

[59] https://www.youtube.com/@RoutingMANRS/featured

MANRS' Virtual Training is More Popular than Ever

A total of 493 trainees were enrolled in MANRS self-paced online tutorials[60] in 2023. The tutorials are available on the MANRS website in English, Spanish, and French. In addition, four in-person trainings on MANRS-related topics were conducted alongside APRICOT (Philippines), BDNOG (Bangladesh), INEX (Ireland), and ZANOG (South Africa).

Continuous Improvement of the MANRS Observatory

The MANRS Observatory,[61] launched in August 2019, is an online tool that monitors Internet routing security by aggregating data from trusted sources into a user-friendly dashboard for viewing routing incidents and checking routing health. The Observatory brings increased transparency to routing operations and sheds light on trends in routing security globally, regionally, and for individual networks so that improvements are made based on evidence.

The MANRS Observatory dashboard gives a high-level overview of the state of routing security, MANRS readiness, and statistics for specific regions and economies. MANRS readiness indicates how well MANRS actions are implemented and is calculated using a set of metrics for each action, computed from different data sources. The Observatory dashboard is open to the public, but MANRS participants can access detailed statistics and conformance reports for their specific networks. Partner accounts are available for individuals or organizations to support research on routing security and efforts in promoting MANRS.

MANRS continues to improve conformance measurements.[62] We have been working with researchers and network operators to improve the data quality and tools.[63] In 2023, we made MANRS Observatory data available via a public API.[64] In addition, we included data on ROA objects and their validation sourced from the MANRS ROA Stats Tool (ROAST),[65] improved the accuracy of the ROAST scores, added RPKI data,[66] improved false positive feedback mechanism, and upgraded underlying technical stack to improve performance and security.

4. Community Spotlight

The MANRS community comprises participants, partners, mentors, and ambassadors. In 2023, the number of MANRS participants crossed the 1,000 mark, with 1,073 participants as of 31 December 2023.

MANRS participants include:

- Network operators that secure customer-provider interconnections.
- Equipment vendors, which make sure network equipment has the right features and support.
- IXPs, CDNs, and cloud providers, which create a secure network peering environment and encourage good routing practices from their members, customers, and partners.

We also have 20 partners who do not necessarily operate networks but actively support MANRS goals. In 2023, the TOP-IX Consortium joined the Internet Society as an organization member, specifically to support MANRS.

---

[60] https://www.manrs.org/resources/training/tutorials/

[61] https://observatory.manrs.org/#/about

[62] https://www.manrs.org/2022/06/configuration-issue-penalizing-single-digit-asns/

[63] https://www.manrs.org/2022/04/rfc-7911-what-happens-when-routers-do-not-speak-the-same-language/

[64] https://www.manrs.org/2023/02/theres-an-api-for-that/

[65] https://www.manrs.org/2023/05/introducing-roast-data-for-the-manrs-observatory/

[66] https://www.manrs.org/2023/10/manrs-observatory-updates-to-provide-3-5-times-more-rpki-data/

Figure 7 Testimonials from MANRS Participants.

The [testimonials](#)[67] from MANRS participants and partners confirm the relevance and importance of MANRS and their recognition of MANRS as a leader in global routing security.

MANRS Mentors and Ambassadors Program

In 2023, [three mentors and eight ambassadors](#)[68] joined the fourth cohort of the [MANRS Mentors and Ambassadors program](#)[69] (formerly the Ambassadors and Fellows program) from June to December.

Mentors are well-respected routing security professionals who provide guidance and feedback to ambassadors working across three tracks—training, research, and policy.

Figure 8 Meet the 2023 MANRS Mentors and Ambassadors.

---

[67] https://www.manrs.org/about/testimonials/

[68] https://www.manrs.org/champions/meet-the-2023-manrs-mentors-and-ambassadors/

[69] https://www.manrs.org/champions/

In 2023, two ambassadors from 2022—Harish Chowdhary and Taejoong (Tijay) Chung—returned as mentors. The APNIC Foundation and APNOG sponsored the 2023 MANRS Mentors and Ambassadors program.

The mentors and ambassadors worked together in their regions and industries to train engineers in routing security best practices, conduct research on detecting incidents, build new tools for the MANRS community, and help policymakers better understand why routing security matters. Collectively, they conducted 20 training events in 8 countries, reaching hundreds of people around the globe. The events were organized in collaboration with NAP Colombia, Kolkata IXP and inSIG 2023 in India, LAC-IX, ANUIES and IXSY in Mexico, PIT Honduras, and others, as well as with Internet Society Chapters in Benin, Colombia, and Dominican Republic.

In addition to the training events, some notable achievements by the mentors and ambassadors included:

- The Zen Guide to BGP Security Policy.[70]

- A research paper on A System to Detect Forged-Origin BGP Hijacks[71] (accepted by the 21st USENIX Symposium on Networked Systems Design and Implementation), and website.[72]

- A research paper on RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI[73] (accepted by the 2023 ACM Internet Measurement Conference), and website.[74]

- New MANRS Observatory tool to visualize the routing security supply chain.

- Data-driven policy recommendations and sector-specific routing security analysis in Pakistan.[75]

- Analysis of the governments' use of routing security in Latin America.

Figure 9 A Selection of Activities Led by MANRS Mentors and Ambassadors.

---

[70] https://www.manrs.org/2023/12/the-zen-guide-to-routing-security-policy/

[71] https://www.manrs.org/wp-content/uploads/2023/12/DFOH_nsdi24.pdf

[72] https://dfoh.info.ucl.ac.be/

[73] https://www.manrs.org/wp-content/uploads/2023/10/Research_RoVista_IMC_2023.pdf

[74] https://rovista.netsecurelab.org/

[75] https://www.manrs.org/2023/12/data-driven-policy-recommendations-and-sector-specific-routing-security-analysis-in-pakistan/

5. Challenges and Lessons Learned

Through some of our in-person MANRS community sessions, we received important feedback that we have used to improve the MANRS initiative. However, the MANRS team can only attend a few events globally in person per year and, therefore, the priority becomes the meetings that will aggregate the most MANRS participants, such as regional Internet registry and network operators group meetings. More in-person engagements will reap greater benefits for the MANRS team and the MANRS community, and a workable model must be sought.

On the policy front, a significant win for routing security in 2023 was the organization of a BGP Security Workshop by the United States FCC that stressed the importance of addressing BGP vulnerabilities. It was welcoming to see many attendees at the workshop mention MANRS and how the MANRS community was setting a new norm for routing security. On the other hand, research indicates that more policy advocacy is needed in many countries, such as India[76] and Pakistan.[77] A key lesson is the importance of policy engagement, which needs to continue to maintain the progress made so far.

To keep the MANR Observatory as current as possible, we rely on various data sources and continuous research into ways of presenting accurate data. This presents multiple challenges, and occasionally, we are informed of incorrect data on the MANRS Observatory, which we try to address quickly. We thank our community for the continuous feedback on ways to improve the Observatory.

6. Looking Ahead

As announced in November 2023, the MANRS secretarial and operational functions will transition[78] to the Global Cyber Alliance starting 1 January 2024. This is an excellent opportunity for MANRS to reach greater heights and be the globally-recognized standard in routing security. The MANRS Steering Committee will continue to be a vital voice of the community and has endorsed the transition.

The Internet Society has funded the MANRS initiative since its inception and will continue to do so for the next five years as part of the transition. This does not negate the need for industry sponsors interested in supporting the MANRS Observatory, the Mentors and Ambassadors program, and the MANRS community events, including the Routing Security Summit. The more support we can generate, the more we can do to secure the global Internet for everyone.

Over the coming year, MANRS will strengthen and add to its best practices, including developing these into recognized standards. As routing security has gained the attention of policymakers, MANRS will also be monitoring and providing inputs where appropriate to regulatory developments as these happen.

We see MANRS continuing to strengthen and the MANRS community continuing to grow with increasing numbers of network operators, IXPs, CDNs, cloud providers, equipment vendors, and partner organizations driving the global adoption of MANRS actions and improvements in routing security.

To our MANRS community, thank you for the trust and support provided to the MANRS initiative over the past ten years, and we look forward to engaging in making the Internet better for all.

---

[76] https://www.manrs.org/2023/03/manrs-compliance-increasing-more-work-needed-in-india/

[77] https://www.manrs.org/2023/12/data-driven-policy-recommendations-and-sector-specific-routing-security-analysis-in-pakistan/

[78] https://www.manrs.org/2023/11/achieving-greater-heights-for-manrs/

MANRS

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative supported by the Internet Society that provides crucial fixes to reduce the most common routing threats.

manrs.org